**IT Applications Unit 3, AOS 1, Online Communities**

1. Complete the following, from pgs, 32: **Network security**

**Networks are classified according to below and we will study the following:**

1. Network Categories: LAN, WAN
2. Network Architecture, client-server; peer-to-peer; internet peer-to-peer; intranet
3. Network communication standards
4. Network hardware and software
5. Transmission media
6. **Network security**
7. What types of physical security measures can be put in place?

Many various security measures are able to be employed when it comes to protecting a network from the outside world. Some of the more common security measures are; Usernames and passwords, Firewalls, virus and malware protection, Encryption and https.

**Usernames and passwords**

1. Recommend a password strategy that an organisation could use to avoid unauthorised access to the network.

Some password strategies to maintain a high level of security include:

1. The password should be at least eight digits long.
2. Include non-alphabetical characters
3. Not be easily guessed (e.g. your password is ‘password’)
4. Be changed every month

**Firewall**

1. Describe the nature of a firewall.

A firewall is a combination of a server and software that filters the information coming through an internet connection into the network. The filters used b a firewall include examining the IP address of computers that request info from an internal server, blocking access to certain domain names, banning certain protocols (e.g. file transfer protocol, mail protocol or Telnet protocol) from accessing certain servers.

1. What are the main purposes of firewalls and how are these purposes achieved?

The main purposes of a firewall are to protect the network from malware that may be trying to access the network from the internet or through wireless connection and in many cases restrict certain users from accessing inappropriate or sensitive material.

1. Why do firewalls use 2 separate NICs?

So that one is connected o the internal network and one to the outside world.

**Malware protection**

1. What is malware and what strategies are used to protect against this type of software?

Malware refers to malicious software and includes spyware, adware, Trojan horses, worms and viruses. Spyware and adware use cookies to track the internet sites that the user visits. Viruses hijack your system and perform various problematic actions.

**Encryption**

1. What is encryption?

Is the process of translating data into a secret code.

1. Describe the nature of WPA or WPA2.

Is a security protocol for use by wireless LANS. It provides security by encrypting data sent over radio waves.

1. What is encrypted data known as?

Unencrypted data is referred to as plaintext and encrypted data is called ciphertext.

**Secure Websites**

1. Describe the secure protocol to allow secure financial transactions across the internet.

The secure protocol is called the **Hypertext transfer protocol security (https)**.

1. What is digital identification certificate technology based on?

It is based on a trust certificate authority such as Verisign Incorperated.

1. Describe the nature of Secure sockets layer (SSL) protocol.

It is a cryptographic protocol that provides secure connection over the internet. When a browser points to a secured domain, a SSL ‘handshake’ authenticates the sever and client.

**Physical design of networks**

1. What is the role of a network diagram?

A network diagram is a schematic method of showing the physical devices and communicates lines present in a network. The diagrams use straight lines to represent cables, and icons are used for communications devices.